

Date

[Policyholder/Claimant Name]

[policyholder/Claimant Address]

Dear [Name]:

We are sending this letter to you as part of the commitment of Paramount Insurance Company, in Receivership, (referenced in this notice as Paramount) to policyholder's, claimant's, and provider's privacy, and to comply with laws, regulations, and other guidance administered by the U. S. Department of Health and Human Services, the state of Maryland, and District of Columbia, Official Code sec. 28-3852. We take the privacy of policyholder, claimant, and provider information very seriously, and it is important to us that you are made fully aware of a potential privacy issue.

On February 19, 2019, at approximately 2:52 pm, EST, we became aware that one terminal server in Paramount's computer system was the target of a ransomware attack. As soon as the attack was discovered, the server was immediately taken off line. All remaining systems were scanned for viruses and malware and found to be free from infection and the systems were restored that evening from a nightly backup. Our investigation found no evidence that information from our system was copied or transferred outside our system. Our investigation also confirmed that Paramount had taken every reasonable precaution to prevent unauthorized access to your personal health information and/or personal information.

Although we have every reason to believe that your personal information was not viewed by an unauthorized person, we are keenly aware of the importance of your personal information. In fact, guidance by the U.S. Department of Health and Human Services provides that in every ransomware attack we must assume that your personal health information was accessed, and provide notice to potentially impacted individuals. Based upon regulatory guidance and our investigation, we have determined that the files that might have been accessed were Paramount electronic files (created between 2008 and the date of the ransomware attack) and potentially contain "protected health information" and/or "personal information", such as your name, social security number, date of birth, home address, phone number account number, diagnosis, disability code, federal issued identification number, or state issued identification number.

We recommend that you take steps to protect yourself from potential information-breach harm. Such steps could include:

- Registering a fraud alert with the three credit bureaus listed here, and ordering credit reports:
 - Experian: (888) 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013
 - TransUnion: (800) 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790
 - Equifax: (800)525-6285; www.equifax.com; P.O. 740241, Atlanta, GA 30374-0241
- Monitoring account statements, explanation of benefits notices, and credit bureau reports closely
- Considering changing passwords, security codes, and security questions and answers on account information provided to Paramount.

Additional information about steps that can be taken to avoid identity theft is available from the Federal Trade Commission (www.ftc.gov), (877) 382-4357, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580 ; the Consumer Protection Division at the Office of the Maryland Attorney General (consumer@oag.state.md.us), (888) 743-0023, 200 St. Paul Place, Baltimore, Maryland 21202.

Paramount Insurance Company, in Receivership, has reviewed its computer security procedures and protections, and has completed an inspection of its premises and computer systems to ensure that all personal health information and personal information is and remains appropriately stored and secured. We regret that this situation has occurred, and we apologize for the inconvenience this poses for you. Paramount Insurance Company, in Receivership, is committed to protecting your personal information.

Sincerely,
William W. Furr, CPCU
President

Leo C. Garrity, Jr.
On Behalf of
Risk & Regulatory Consulting LLC,
As Receiver